Patch Release Note

Patch 54266-02
For AR440S and AR441S ADSL Routers

Introduction

This patch release note lists the issues addressed and enhancements made in patch 54266-02 for Software Release 2.6.6 on existing models of AR440S and AR441S ADSL routers. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 54266-02.

Base Software Release File	54-266.rez
Patch Release Date	9-Dec-2004
Compressed Patch File Name	54266-02.paz
Compressed Patch File Size	246872 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.6.6 for AR440S ADSL Routers (Document Number C613-10412-00) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- AR400 Series router Documentation Set for Software Release 2.6.6 available on the Documentation and Tools CD-ROM packaged with your router, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Errata to the Documentation: Software Release 2.6.6 for AR440S ADSL Routers (Document Number C613-06011-00) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

From Patch 54266-02 onwards, issues for each patch are listed in severity order as per the levels above. Enhancement PCRs are listed after Level 4 issues.

Features in 54266-02

Patch 54266-02 includes the following enhancements and resolved issues:

Level 1

PCR: 40660 Module: ATM Level: 1

When an L2TP call was activated over any ATM link (PPPoA, PPPoEoA, IPoA e.t.c.) a router reboot would occur. This issue has been resolved.

Level 2

PCR: 40266 Module: IPSEC Level: 2

Out of sequence IPSEC packets could cause a router reboot. This issue has been resolved.

PCR: 40272 Module: IPG Level: 2

The router learned an ARP entry for an IP address that was already configured on one of its interfaces. This issue has been resolved, and the receipt of spoofed ARP packets will now generate a log message.

PCR: 40284 Module: PIM Level: 2

When PIM-SM was configured and a very large number of IGMP v2 joins were received, a router reboot would occur. This issue has been resolved.

PCR: 40311 Module: IPG Level: 2

A router reboot was observed when a large number of IP flows were being deleted when an interface went down. This issue has been resolved.

PCR: 40419 Module: OSPF, IPG Level: 2

If OSPF was configured using the command **set ospf dyninterface=stub,** to advertise dynamic interfaces such as PPPoE interfaces as stub links, the links were not being advertised as expected. This issue has been resolved.

PCR: 40442 Module: IPSEC Level: 2

When an IPSEC policy is used on a PPP link with **iprequest=on**, when the PPP link goes down and IPSEC has traffic to transmit, IPSEC repeatedly attempts to activate the PPP link again. The frequency of the reactivation attempts has been reduced.

PCR: 40446 Module: DHCP Level: 2

In certain situations, if a DHCP client used a DHCP relay agent to request IP addresses from the router acting as the DHCP server on a different subnet, it was not be able to renew the IP address allocated to it. This issue has been resolved.

PCR: 40450 Module: IPG Level: 2

IGMP entries were sometimes changed to static entries rather than being deleted when IGMP leaves were received. This issue has been resolved.

PCR: 40451 Module: FIREWALL Level: 2

The "number of hits" counter in firewall's application rules was not incremented correctly. This issue has been resolved.

PCR: 40453 Module: PIM Level: 2

Particular IP packets (unicast destination IP, but multicast destination MAC) could result in a memory leak, which in some cases could cause the device to stop responding to the command line. This issue has been resolved.

PCR: 40456 Module: IPG Level: 2

The **enable switch learning** command would fail if 802.1X port authentication was enabled on any of the switch ports. This issue has been resolved.

PCR: 40458 Module: IPG Level: 2

The router was accepting network RIP packets from foreign subnets. This issue has been resolved.

PCR: 40465 Module: PIM6, PIM4 Level: 2

The router could reboot when a user changed the Rendezvous Point Candidate (RPC) priority in the PIM6 module. This issue has been resolved.

PCR: 40466 Module: ISAKMP Level: 2

When the router was the initiator in an ISAKMP Quick mode exchange with a PC running Windows 2000 or Windows XP, the IPSEC communication would not establish successfully. This was because the Windows PC set the commit bit in the exchange, but sent the CONNECTED Notify payload in the Quick mode exchange. However, the router was waiting for an Informational Exchange containing a Notify payload (with the CONNECTED Notify Message) as specified by RFC 2408. Because an Informational message was expected, the device did not process the Quick mode CONNECTED message, and so the exchange was never committed.

Although this behaviour is described as "not required by the IKE standard" [http://www.microsoft.com/technet/community/columns/cableguy/cg0602.mspx], the device will now process CONNECTED messages received in Quick mode exchanges, to allow interoperability with other vendors.

PCR: 40470 Module: BGP Level: 2

When BGP redistributed routes, locally imported routes were selected rather than peer learnt routes. This issue has been resolved.

PCR: 40479 Module: OSPF Level: 2

For OSPF-originated routes, it was possible for a route to be deleted from the IP routing table, but still be referenced by OSPF. This could cause a router reboot when later generating a summary LSA that contained the old route. This occurred using the **reset ip** command. This issue has been resolved.

PCR: 40496 Module: DHCP Level: 2

When DHCP is enabled, it reclaims IP addresses at router startup to determine if the addresses are in use or not. If, during this process, DHCP was disabled then re-enabled, the router would not attempt to reclaim the remaining IP address ranges. This would lead to the rejection of DHCP requests for IP addresses that were still being reclaimed. This issue has been resolved.

PCR: 40516 Module: DHCP Level: 2

While initialising a range, the router acting as a DHCP server may release a dynamic entry incorrectly. This issue has been resolved.

PCR: 40520 Module: DVMRP Level: 2

Multicast data could not flow from PIM to DVMRP on a PIM/DVMRP border router. This issue has been resolved.

PCR: 40530 Module: IPG Level: 2

When both Load Balancer and Firewall were configured, the very first TCP session was established after rebooting. Subsequent TCP session startup packets may have been routed out to an incorrect interface causing sessions to not be established. This issue has been resolved.

PCR: 40537 Module: BGP Level: 2

When the status of an interface changed, the BGP revaluation of IP routes for redistribution (via the **add bgp import** or **add bgp network** commands) was incorrect. This gave inconsistent BGP route tables depending on the order of events. This issue has been resolved.

PCR: 40549 Module: SWI Level: 2

The receipt of two IP packets whose destination IP addresses were subnet addresses caused the router to reboot. This issue has been resolved.

PCR: 40560 Module: DHCP Level: 2

A router reboot could occur when the DHCP server checked whether an IP address was being used by other hosts, for example, after processing a DHCP Discover message. This issue occurred if **probe=arp** was specified for the DHCP range, and if DHCP had been disabled and then enabled. This issue has now been resolved.

PCR: 40573 Module: LOG Level: 2

If the log module was configured to store a very large number of messages (for example, more than 3000 messages), a watchdog timeout could occur when the **show debug** command was executed. This issue has been resolved.

PCR: 40587 Module: IPG, PIM, DVMRP Level: 2

When doing Layer 3 IP multicast routing, the router would flood traffic to all ports in the downstream VLAN. This issue has been resolved, and now the router will do the portmap calculation based on IGMP, PIM-SM, PIM-DM, DVMRP neighbour information, and forward the multicast traffic to the calculated portmap.

PCR: 40588 Module: PPP, CC Level: 2

A toplogy change in a network could cause a router to attempt to activate an ISDN call configured with direction=in when the call was already activated. In this situation, the call was failing, and the PPP link over the call would not come open. This issue has now been resolved.

PCR: 40592 Module: BOOTP Level: 2

If a timed-out ARP entry was renewed by BOOTP, the new entry be created with no port association. This issue has been resolved.

PCR: 40599 Module: FIREWALL Level: 2

The **add firewall apprule** command did not correctly accept the **port** parameter, so the port value was set to zero. This issue has been resolved, and the port value is stored correctly.

PCR: 40612 Module: IPG, DNS Relay Level: 2

There was an issue in DNS Relay that resulted in a memory leak. The leak occurred when a response to a relayed DNS request contained an authoritative nameserver or additional information and the DNS request was forwarded to one of those servers. There was also an issue whereby DNS queries handled by DNS Relay would sometime result is corrupt entries in the DNS cache. These issues have been resolved.

PCR: 40621 Module: PING Level: 2

In previous releases, ping poll commands only required entry of the first three characters of the Source IP Address (**sipaddress**) parameter. For example, **add ping poll=1 ip=192.168.2.10 sip=192.168.2.1**. Subsequent releases required entry of the first four parameters. This issue has been resolved, so that it is once again possible to enter just the first three characters.

PCR: 40646 Module: OSPF, IPG Level: 2

For both RIP and OSPF, the router was adding a route with it own IP address for NEXTHOP address. This issue has been resolved.

PCR: 40658 Module: L2TP Level: 2

L2TP did not handle a change to its peer's UDP source port. If the tunnel went through a NAT box and that NAT box was reset, then it was possible for the remote port to change. L2TP should be able to handle this case and update the tunnel accordingly. A similar problem occurs when a IPsec NAT-T session (in transport mode) is re-negotiated. IPsec NAT-T uses port translation to distinguish between multiple clients behind a NAT box. If the IPsec session is renegotiated then the translated source port that IPsec passes to L2TP will change. L2TP must be able to handle this case, if it doesn't then the session will be lost. This issue has been resolved.

PCR: 40668 Module: FFILE Level: 2

The router would not respond to the setting of the **maxqueueseverity** parameter when configuring logging. This issue has been resolved.

PCR: 40728 Module: IPNAT Level: 2

When IP NAT was configured, a router reboot could occur if a TCP RST packet was received in which the ACK flag and at least one other flag had been set. This issue has been resolved.

Level 3

PCR: 31225 Module: IPG Level: 3

While the router was set with a CIDR interface address, when it received an ECHO request with a network broadcast destination address for a class C network, the router sent the ECHO reply packet. Also, the router forwarded the ECHO request packet using a broadcast MAC address. These issues have been resolved.

PCR: 40417 Module: OSPF Level: 3

When LS Acks (Link State Advert acks) were received, they were compared against the transmitted LSA (Link State Advert). If it was the same, the LSA was removed from the re-transmission list. The algorithm used in this check has been changed to be compliant with the algorithm specified in section 13.1 of RFC2328, to determine if the LS Ack received is the instance as the LSA.

PCR: 40428 Module: IP, FILTER Level: 3

If the value specified for the **sport** or **dport** parameter in the **add ip filter** or **set ip filter** commands was 65535, then the IP filter process would incorrectly interpret that value as meaning “any “ port. This issue has been resolved so that port 65535 is now used for the IP filter when specified.

PCR: 40437 Module: CORE Level: 3

The tick timer was not initialised correctly, which could cause firewall sessions to time out prematurely when the system time reached midnight. This issue has been resolved.

PCR: 40493 Module: DHCP Level: 3

In certain scenarios when acting as a DHCP server, the switch would send a DHCP ACK to an invalid MAC address. This issue has been resolved.

PCR: 40498 Module: OSPF Level: 3

When a virtual link end point is no longer reachable, the virtual interface is not brought down, and the virtual neighbour is not removed. This issue has been resolved.

PCR: 40513 Module: PIM6 Level: 3

The RP Candidate address was not displayed correctly when issuing the "**show pim6 rps**" command. This issue has been resolved.

PCR: 40610 Module: BRIDGE Level: 3

When the **set bridge port** command was executed, the bridge configuration resulting from the **create config** or **show config dynamic=bridg**e commands would be incorrect. This issue has been resolved.

PCR: 40676 Module: ADSL, CORE Level: 3

The ADSL interface, adsl0, did not appear in the Interface Name Summary table section of the **show interface** command output or in the **arInterfaceTable** in the Allied Telesyn enterprise MIB. This issue has been resolved.

Level 4

PCR: 40441 Module: IPG, VRRP Level: 4

If VRRP was enabled and a **reset ip** command was issued followed by a **disable vrrp** command, then the device would still reply to pings, even though the device was no longer the VRRP master. Duplicate echo replies were seen on the device sending the pings. This issue has been resolved.

Enhancements

PCR: 40521 Module: TACACS+

The new command **show tacplus** has been added. This command shows the module status, number of servers, and number of logged in users.

PCR: 40677 Module: ADSL

The new ADSL Annex B firmware has been incorporated to allow compliance with UR-2 specifications.

AR441S ADSL Router Hardware Platform

Patch 54266-01 includes support for the AR441S ADSL (Annex B) router.

Each AR441S router consists of a base CPU card, enclosure, and power supply. The base CPU card supports:

- One Asymmetric Digital Subscriber Line (ADSL) Annex B port.
- Five 10/100 LAN switch ports.
- One asynchronous RS-232 (ASYN0) port.

The PIC bay can accommodate any of the following PICs:

- AT-AR020 PRI E1/T1 PIC, one Primary Rate E1/T1 port.
- AT-AR021(S) BRI-S/T PIC, one Basic Rate ISDN S/T port.
- AT-AR021(U) BRI-U PIC, one Basic Rate ISDN U port.
- AT-AR022 ETH PIC, one Ethernet LAN AUI/10BASE-T port.
- AT-AR023 SYN PIC, one Synchronous port with universal 50-way AMPLIMITE connector.
- AT-AR024 ASYN4 PIC, four Asynchronous ports with RJ-45 connectors.
- AT-AR026 4ETH PIC, four 10BASE-T/100 BASE-TX auto-negotiating ports with RJ-45 connectors.
- AT-AR027 VoIP-FXS PIC, two Foreign Exchange Subscriber (FXS) ports with RJ-11 connectors.

Main system

Main features of the AR440S routers are:

- 300 MHz RISC processor.
- 64 MBytes of SDRAM.
- 16 MBytes of flash memory (1 MByte reserved for boot block code).
- 5 x 10/100 Mbps full duplex, Layer 2 switched Ethernet LAN ports. All LAN ports have Auto-MDI, however if Auto-MDI is turned off, then all ports are hardwired as MDI-X. Software can also force a port to either MDI or MDI-X. 802.1Q tagged VLANs are supported.
- 1 x ADSL Annex B port
- 1 x asynchronous DTE port.
- Universal AC power supply.
- On-board hardware encryption processor for DES, 3DES and AES.

Some encryption options may require feature licenses.

The RS-232 asynchronous serial port (ASYN 0) has a DB9 male connector, is wired as a DTE port and can be used as a general purpose port for terminals, printers or modems. The default communications settings are:

- 9600 bps
- 8 data bits
- 1 stop bit
- no parity
- hardware flow control

ADSL Interfaces

The ADSL port has an RJ11 connector, and supports Dying Gasp.

Power supply

The routers have a universal AC input connector and a power switch on their rear panel. The routers require a power input of 100-240 VAC and 50–60Hz.

Some interfaces that may be installed in the router are not transformer isolated. This means they will be referenced to the frame ground of the equipment and may be damaged if connected to an interface on another piece of equipment which is at a different ground potential.

For more information about the hardware, see the *AR400 Series Hardware Reference* on the *Documentation and Tools CD-ROM*.

Features in 54266-01

Patch file details are listed in Table 2.

Table 2: Patch file details for Patch 54266-01.

Base Software Release File	54-266.rez
GUI Resource File Names	d440Se14.rsc (AR440S) d441Se14.rsc (AR441S)
Patch Release Date	21-Oct-2004
Compressed Patch File Name	54266-01.paz
Compressed Patch File Size	161304 bytes

Patch 54266-01 includes the following enhancements and resolved issues:

PCR: 40563 Module: ADSL

This patch, together with the base software release, supports the AR441S ADSL (Annex B) router. With this patch, the AR440S ADSL port operates in Annex A mode for ADSL over POTS, and the AR441S ADSL port operates in Annex B mode for ADSL over ISDN. ("AR441S ADSL Router Hardware Platform" on page 8)

PCR: 40568 Module: SWK Level: 3

If the Jabber counter in the output of the **show switch port counter** command had more than four digits, it displayed an incorrect value. This issue has been resolved.

PCR: 40572 Module: M8272 Level: 3

An AR023 synchronous port interface card (PIC) installed in an AR440S failed the Test facility interface test, even when there was nothing wrong with the PIC. This issue has been resolved.

PCR: 40576 Module: Firewall Level: 2

When the firewall was creating new NAT entries under extremely heavy loads, it occasionally caused a fatal error. This issue has been resolved.

PCR: 40581 Module: BRG Level: 2

The router could not bridge between an ATM channel and a VLAN interface. This issue has been resolved.

PCR: 40582 Module: BRG Level: 2

Occasionally a reboot occurred when the router attempted to bridge traffic to an ATM channel before the channel had come up for the first time. This issue has been resolved.

PCR: 40585 Module: IPG Level: 2

Attaching an IP interface to a VCMux encapsulated ATM interface with Inverse ARP disabled by using the command:

```
add ip interface=atm0.1 ipaddress=192.168.1.1
   inversearp=off
```

failed, giving one of the messages:

```
Error (3005271): Internal Error: Failed to start interface
```

```
Error (3005271): Internal Error: Failed to set interface
```

This issue has been resolved. It is now possible to add an IP address to a VCMux encapsulated ATM interface with **inversearp** set to **off**. This is known as RFC 1483 routing. RFC 1577, classical IP and ARP over ATM, still requires the ATM interface to be LLCSNAP encapsulated.

PCR: 40613 Module: SYN Level: 3

When the Test facility was used to test an AR023 synchronous PIC interface, it sent some debugging messages, "SYNCheckInterface", to the console port. This issue has been resolved: the Test facility no longer sends these messages.

PCR: 40618 Module: Firewall Level: 3

When NAT was enabled and the router was configured to pass FTP requests to a server inside the network, the Firewall translated the ftp-data source port (tcp/20) of an FTP server located on a private interface to another port. Such packets no longer conformed strictly to RFC 959, and some other firewalls on the Internet may then have denied them. This issue has been resolved: the Firewall now sends all ftp-data packets from port 20 on the firewall, whether or not NAT is enabled.

PCR: 40619 Module: IPG Level: 2

The output of the **show config dynamic** command incorrectly displayed the following parameters for the **set ipv6 prefix** command, even when they were not specified with the command:

- The **valid** parameter displayed an incorrect value; the router did not use this incorrect value.
- The **preferred** parameter displayed an incorrect value; the router did not use this incorrect value.
- The **onlink** parameter displayed the default value **yes**.
- The **autonomous** parameter displayed the default value **on**.

This issue has been resolved: the unused parameters are no longer displayed.

PCR: 40625 Module: SWK Level: 2

The GUI on the AR441S did not display a port map on the System Status page. This issue has been resolved. GUI resource file **d441Se14.rsc** or later is also required to display the port map on the AR441S.

PCR: 40629 Module: Firewall Level: 2

A fatal exception in the firewall occurred occasionally when a large number of proxied connections were rapidly established, for example, during a SYN attack. This issue has been resolved.

PCR: 40633 Module: ENCO Level: 2

The encryption engine on the AR441S was not initialised. 3DES outer, 3DES inner and AES encryption algorithms were not available. This issue has been resolved.

PCR: 40638 Module: Firewall Level: 2

When a global interface was dynamically assigned an IP address via DHCP or PPP, NAT configurations with dynamic private interfaces (**interface=dyn-<*dyn-int-name*>**) were not updated. This resulted in the failure of sessions received on dynamic private interfaces because the global IP address was invalid. This issue has been resolved.

PCR: 40647 Module: ETH Level: 2

When a virtual Eth interface was created over ATM, for example, using the command:

```
create eth=0 over=atm=0.1
```

and a VPN configuration was applied directly to that Eth interface, the router ran out off buffers and caused a fatal exception under heavy reception load.

This issue has been resolved: a limit has now been set so that the virtual Ethernet interfaces, like physical Eth interfaces, stop reception by dropping excess packets when the ethernet receive queue is too long or when the router is running out of buffers. The ifInDiscards counter, displayed in the output of the **show eth counter** command, is incremented when this happens on a virtual Eth interface.